配置入侵策略和签名配置在Firepower模块(在箱上管理)

目录

简介

制订在FirePOWER模块的检测策略的本文描述FirePOWER模块的入侵防御系统(IPS) /Intrusion检测系统(IDS)功能和多种入侵策略的元素。

先决条件

要求

Cisco 建议您了解以下主题：

*可适应安全工具(ASA)防火墙知识，可适应安全设备管理器(ASDM)。

* FirePOWER设备知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

运行软件版本5.4.1的ASA FirePOWER模块(ASA 5506X/5506H-X/5506W-X， ASA 5508-X， ASA 5516-X)和更加高。

ASA FirePOWER模块(ASA 5515-X， ASA 5525-X， ASA 5545-X， ASA 5555-X)运行软件版本6.0.0和更加高。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息

FirePOWER IDS/IPS设计检查网络流量和识别指示网络/系统攻击的所有有恶意的模式(或签名)。FirePOWER模块在IDS模式在轴向模式工作，如果ASA的服务策略在监控模式特别地配置(混乱)，它工作。

FirePOWER IPS/IDS是一基于签名的检测方法。 在IDS模式的FirePOWERmodule生成警报，当签名匹配恶意流量时，而在IPS模式的FirePOWER模块生成警报和块恶意流量。

FirePOWER**Configuration> ASA FirePOWER Configuration>**

配置

步骤1.配置入侵策略

步骤1.1。创建入侵策略

要配置入侵策略，请登陆给可适应安全设备管理器(ASDM)并且完成这些步骤：

步骤1.导航对**Configuration> ASA FirePOWER Configuration>策略>入侵策略>入侵策略**。

步骤2.点击**创建策略**。

步骤3.输入入侵策略的**名称**。

步骤4.输入入侵策略的**说明**(可选)。

步骤5.指定**丢弃，当轴向**选项。

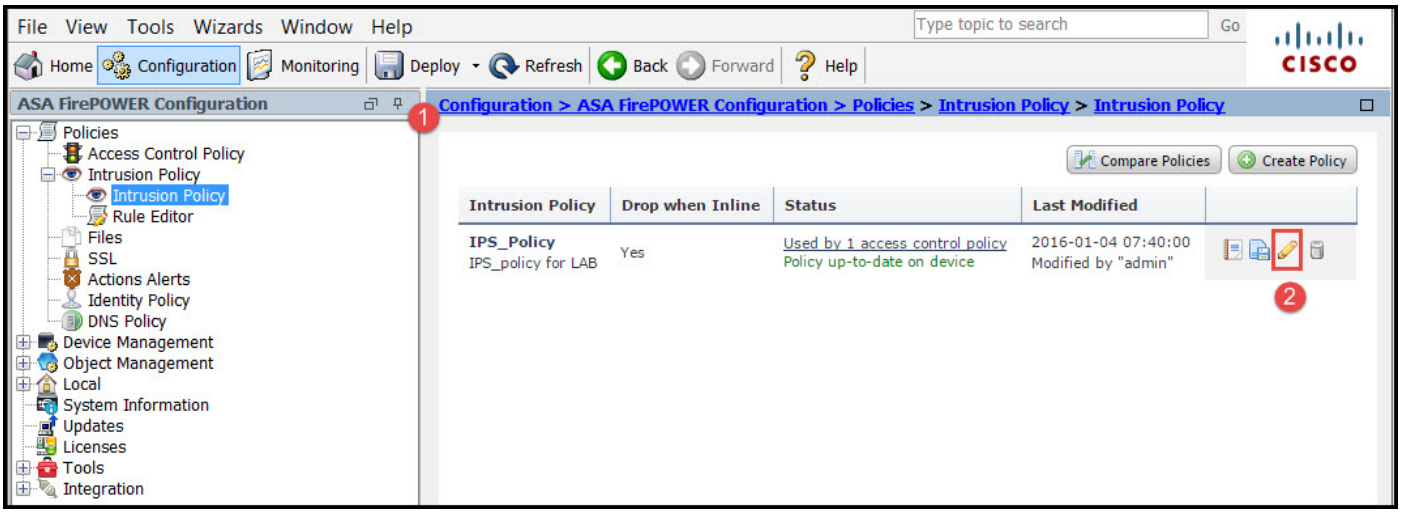
步骤6.选择从丢弃下来列表的**基本策略**。

步骤7.单击**创建策略**完成入侵策略创建。

您能注意策略配置，然而，没有应用到任何设备。

步骤1.2。修改入侵策略

要修改入侵策略，请导航对**Configuration> ASA FirePOWER Configuration>策略>入侵策略>入侵策略**并且选择**Edit选项**。

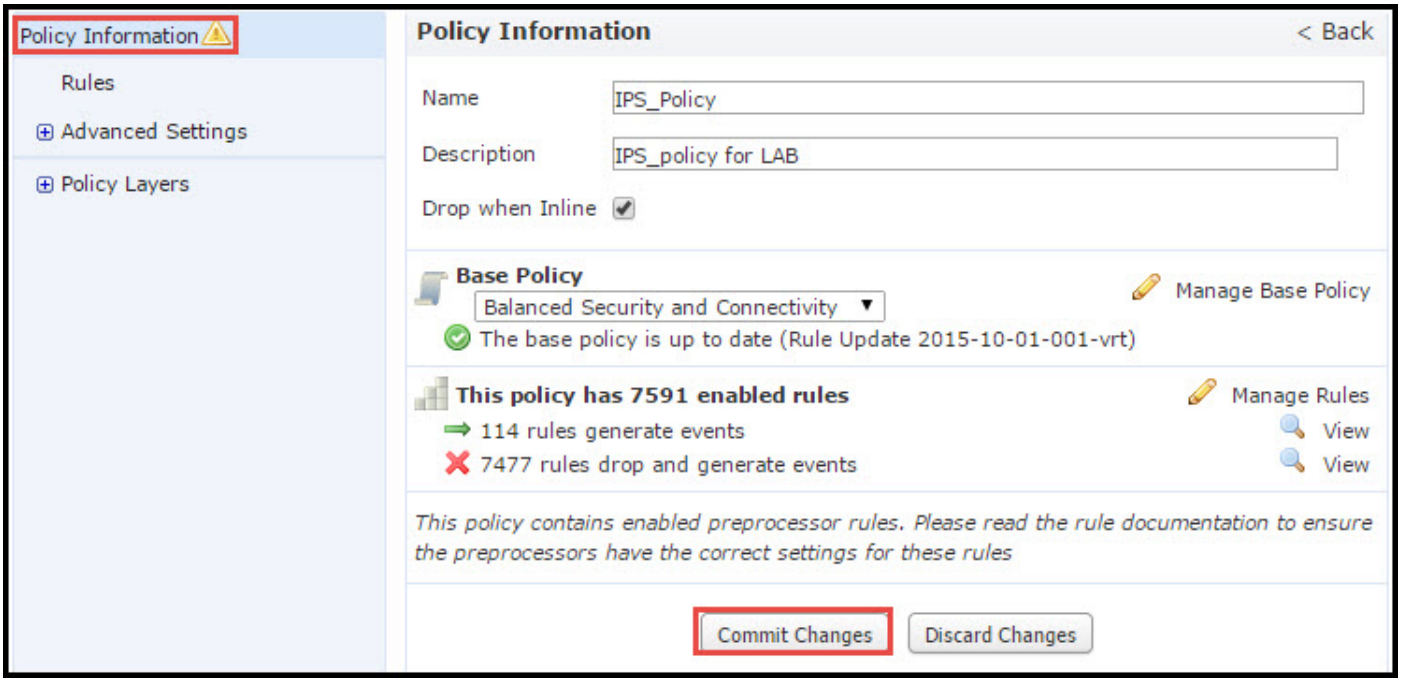


步骤1.3。修改基本策略

入侵策略管理页给出选项更改基本策略丢弃，当线型保存并且丢弃选项。

基本策略包含一些系统提供了策略，是内置的策略。

1. 平衡安全和连接： 它是一项最优策略根据安全和连接。此策略有大约启用的7500个规则，有些只生成事件，而其他生成事件以及降低流量。
2. 在连接的安全：如果您的首选是安全那么您能选择在连接策略的安全，增加已启用规则数量。
3. 在安全的连接： 如果您的首选是连接而不是安全那么您能选择在将减少已启用规则数量的安全策略的连接。
4. 最大检测-选择此策略获得最大检测。
5. 没有规则激活-此选项禁用所有规则。您需要启用规则手工根据您的安全策略。



步骤1.4。与过滤器柱状图选项的签名过滤

导航对**规则**选项在可定位面板中，并且规则管理页出版。有规则的千位在规则数据库的。过滤柱状图提供一个好搜索引擎选项有效搜索规则。

您能插入所有关键字到过滤器柱状图，并且系统获取您的结果。如果有需求查找安全套接字协议层(SSL) heartbleed漏洞的签名，您能在过滤器柱状图和它heartbleed的Search关键字取指令heartbleed漏洞的签名。

> **提示**： 如果多个关键字用于过滤器柱状图那么系统结合他们使用，并且创建复合的逻辑搜索。

通过使用签名ID (SID)，您能也搜索规则，生成器ID (GID)，类别：dos等。

规则有效分开成多种方式例如基于类别分类Microsoft的漏洞/平台特殊化Microsoft的蠕虫。规则的这样关联帮助客户获得在简单的方法的正确签名和帮助客户有效调整签名。

您能用CVE编号也搜索查找包括他们的规则。您能使用语法**CVE ：<cve-number>。**

步骤1.5。配置规则状态

导航对**规则**选项在可定位面板中，并且规则管理页出版。选择规则并且选择选项规则**状态**配置规则的状态。有可以为规则配置的三状态：

1. **生成事件：**当规则匹配流量时，此选项生成事件。

2. **下降并且生成事件：** 当规则匹配流量时，此选项生成事件和丢弃流量。

3. **禁用：**此选项禁用规则。

步骤1.6。 事件过滤器配置

入侵事件的重要性可以频率出现，或者根据来源或目的IP地址。有时，您不可以对事件关心，直到发生一定数量的次。例如，您也许不关系到，如果某人尝试登陆到服务器，直到他们出故障一定数量的次。在某些情况下，您也许只需要看到规则命中数一些出现检查是否有一普遍问题。

有您能达到此的两种方式：

1. 事件阈值。

2. 事件抑制。

事件阈值

您能设置指明的阈值事件多频繁显示，根据出现数量。您能配置门限每个事件和每项策略。

配置事件阈值的步骤：

步骤1.选择您要配置事件阈值的**规则**。

步骤2.点击**事件过滤**。

步骤3.点击**阈值**。

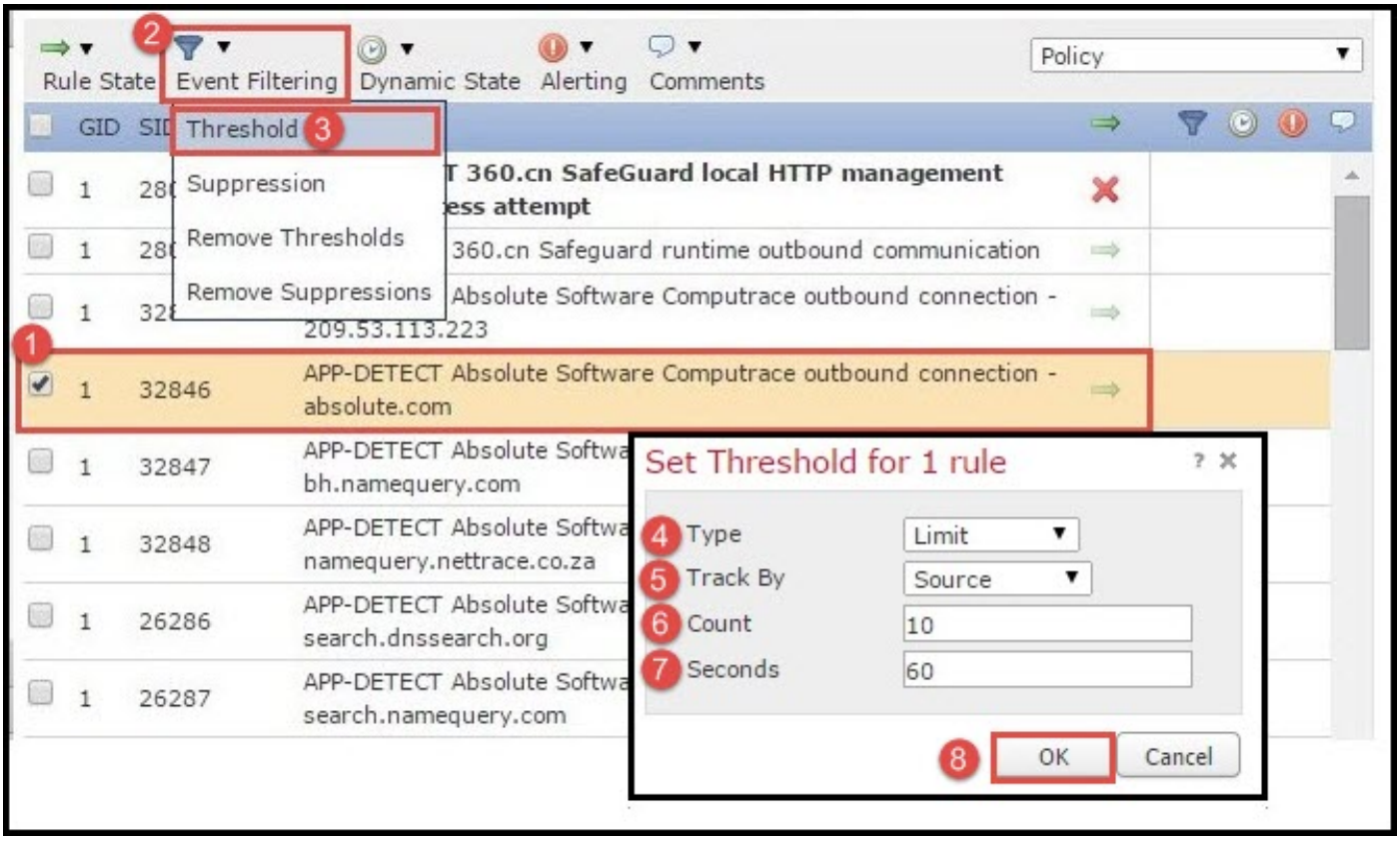
步骤4.选择从丢弃下来列表的**类型**。(限制或阈值或者两个)。

步骤5.选择您如何要从**跟踪**跟踪**由**丢弃方框。(来源或目的地)。

步骤6.进入事件**计数**满足阈值。

步骤7.，在计数重置前，请输入**秒钟**流逝。

步骤8.点击OK键完成。



在事件过滤器被添加到规则后，您应该能在规则征兆旁边发现过滤器图标，显示有为此规则启用的事件过滤。

事件抑制

指定的事件通知可以被抑制根据源/目的地IP地址或每个规则。

注意：当您添加规则的事件抑制。如果流量匹配签名，签名检查工作作为通常，然而系统不生成事件。如果指定一个特定来源/目的地那么事件没仅为特定来源/目的地出现此规则的。如果选择抑制完整规则那么系统不生成此规则的任何事件。

配置事件阈值的步骤：

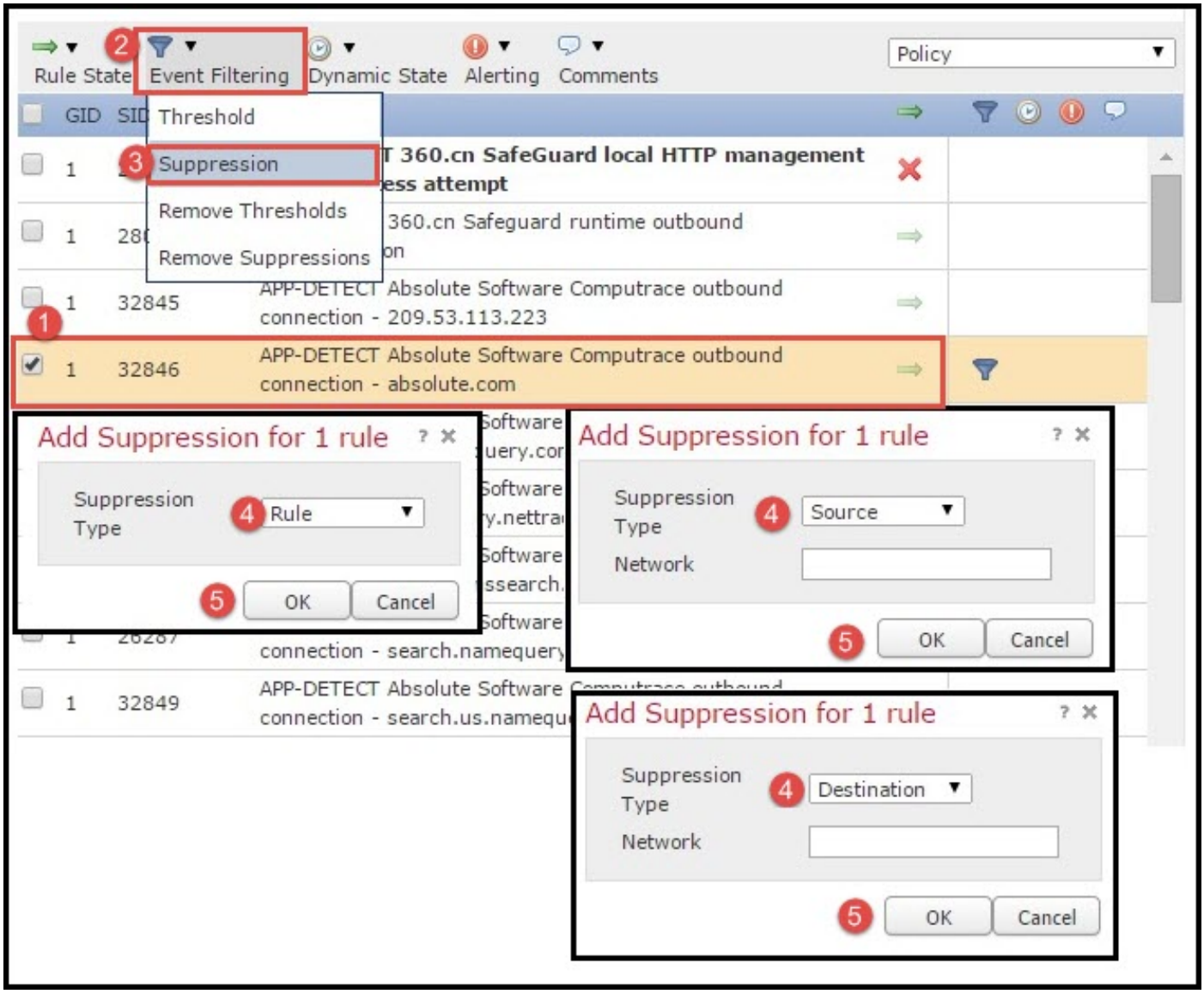
步骤1.选择您要配置事件阈值的**规则**。

步骤2.点击**事件过滤**。

步骤3.点击**抑制。**

步骤4.Select从下来丢弃列表的**抑制类型。**(规则或来源或者目的地)。

步骤5.点击OK键完成。



在事件过滤器被添加到此规则后，您应该能在规则征兆旁边发现与计数两的一个过滤器图标，显示有为此规则启用的两个事件过滤器。

步骤1.7。配置动态状态

它是功能，我们能更改规则的状态specified conditions below是否配比。

假设暴力攻击方案破解密码。如果签名检测密码失败尝试和规则操作是生成事件。系统继续进行生成密码失败尝试的警报。对于此情况，您能使用**Generate事件**操作可以更改**下降和生成事件**拦截暴力攻击的**动态状态**。

导航对**规则**选项在可定位面板中，并且规则管理页出版。选择您要启用动态状态和选择选项**动态状态>Add速率BASE规则状态的**规则。

配置基于速率的规则状态：

1. 选择您要配置事件阈值的**规则**。
2. 点击**动态状态**。
3. 点击**添加基于速率的规则状态**。
4. 选择您如何要**由**丢弃方框跟踪从**跟踪的**规则状态。(**规则或来源或者目的地**)。
5. 进入**网络**。您能指定单个IP地址、地址块、变量或者包括这些的所有组合的一逗号分隔的列表

。
6. 以秒钟进入事件**计数**和时间戳。
7. 选择**新状态**，您要为规则定义。
8. 输入**超时**，在后规则状态被恢复。
9. 单击 OK 完成操作。

步骤2.配置网络分析策略(NAP) &设置的变量(可选)

Configure network分析策略

亦称网络访问策略是预处理程序。预处理程序执行信息包重组并且规范化流量。它帮助识别在不相应的报头选项的识别的网络层和传输层协议反常现象。

NAP执行IP数据包、提供TCP状态检测和数据流重组的坚固和验证校验和。 预处理程序规范化流量，验证并且验证协议标准。

每个预处理程序有其自己的GID编号。它代表哪个预处理程序由数据包触发了。

对configure network分析策略，请导航对**Configuration> ASA FirePOWER Configuration>策略>访问控制策略>Advanced >网络分析和入侵策略**

默认网络分析策略是最优策略的平衡安全和连接。有可以从下拉列表选择的其他另外三项系统提供的NAP策略。

创建自定义NAP策略的挑选选项**网络分析策略**列表。

配置设置的变量

设置的变量用于入侵规则识别源地址和目的地址和端口。当变量更加准确地时，反射您的网络环境规则更加有效。变量播放在性能调整的一重要的角色。

设置的变量已经配置与默认选项(网络/端口)。如果要更改默认配置，请添加新的设置的变量。

要配置设置的变量，请导航对**Configuration> ASA Firepower Configuration>对象Management>设置的变量**。挑选选项**添加设置的变量**添加新建的设置的变量。输入设置的变量**名称**并且指定**说明。**

如果任何定制应用在一个特定端口工作然后定义在Port Number字段的端口号。配置网络参数。

$Home_NET指定内部网络。

$External_NET指定外部网络。

步骤 3：配置访问控制包括入侵策略NAP设置的变量

导航对**Configuration> ASA Firepower Configuration>策略>访问控制策略。**您需要完成这些步骤：

1. 编辑您想要分配入侵策略的访问策略规则。
2. 选择**检查**选项卡**。**
3. 从丢弃下来列表选择**入侵策略**并且从丢弃下来列表选择**设置的变量**

4. 单击 Save。

因为入侵策略被添加到此访问策略规则。您能看到在表明的金黄颜色的屏蔽材料图标入侵策略启用。

点击**存储ASA FirePOWER更改**保存更改。

步骤4.实施访问控制策略

现在，您必须实施访问控制策略。在您运用策略前，您将看到征兆访问控制策略过时在设备。 部署对传感器的更改：

1. 单击**部署**。
2. 单击**部署FirePOWER更改**。
3. 单击**部署**在弹出窗口。

5.4.xASA FirePOWER

Monitoring> ASA Firepower Monitoring>

步骤5.箴言报入侵事件

要看到FirePOWER模块生成的入侵事件，请导航对**Monitoring> ASA FirePOWER Monitoring>实时Eventing。**

验证

当前没有可用于此配置的验证过程。

故障排除

步骤1:保证规则的规则状态适当地配置。

第二步：保证正确IPS策略在访问规则包括的那。

第三步：保证设置的变量正确地配置。如果设置的变量没有正确地配置那么签名不会匹配流量。

第四步：保证访问控制策略部署成功地完成。

步骤5.，如果通信流点击正确规则，请监控连接事件和入侵事件验证。

- **ASA FirePOWER**
- **- Cisco Systems**